

**Annual 47 CFR § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: 2/20/2018
2. Name of company(s) covered by this certification: ICON Technologies Inc.
3. Form 499 Filer ID: **831983**
4. Name of signatory: Alex Kelly
5. Title of signatory: VP/Engineering
6. Certification:

I, Alex Kelly, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions against data brokers in the past year

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Alex Kelly 2/20/18  
Alex Kelly

**Attachments:** Accompanying Statement explaining CPNI procedures

**Attachment "A"**  
**ICON Technologies Inc.**  
**Statement of CPNI Compliance Procedures**

This statement details ICON Technologies Inc's ("ICON's") policy, practices and procedures to ensure compliance with FCC CPNI Rules.

- 1) ICON uses CPNI only to market service offerings that are within the same category of service that is already provided to the customer and, therefore, does not require customer approval pursuant to 47 CFR §64.2005.
- 2) ICON does not disclose CPNI over the phone or provide online access to CPNI.
- 3) ICON does not sell data, including CPNI data, to any third party entity.
- 4) ICON has no affiliates with which to share information.
- 5) Customer requests for CPNI must be made in person and require a government issued photo ID.
- 6) CPNI requests from law enforcement must include a subpoena or court order, which is reviewed by outside council prior to release of the information.
- 7) ICON maintains a written record of all instances where CPNI was provided for a minimum of 1 year.
- 8) ICON maintains a CPNI compliance manual. Employees are retrained on CPNI compliance annually, and new hires are trained as part of the onboarding process.
- 9) The servers which house CPNI data are protected by industry standard firewalls, which include active security update subscriptions and intrusion monitoring systems.
- 10) Backups of CPNI data are encrypted.
- 11) Transmission of CPNI data, including download from wholesale carriers, is encrypted.
- 11) In case of breach resulting in CPNI disclosure, ICON notifies appropriate government agencies, including the US Secret Service and FBI as specified in the FCC CPNI rules. Customers are notified once law enforcement notifications are complete.
- 12) ICON maintains a disciplinary process that specifies that willful violation of CPNI procedures will result in employee termination. Accidental violations result in a written warning, which may lead to termination if repeated.
- 13) ICON maintains a copy of all marketing campaigns for a minimum of one year. Marketing campaigns require approval by an officer of the company.

Signed

  
Alex Kelly